Key Points from the Attached Comment Letter to the ICO to Enable Data Processing for Direct Marketing

Lawful & Ethical Direct Marketing Under GDPR

- Direct marketing processing is often too complex to explain in a way that data subjects can provide informed and sufficient consent. This means that Pseudonymisation and Data Protection by Design and by Default - *as newly defined for the very first time at the EU level in the GDPR* - are the only viable options for this kind of processing to be lawful and ethical.

Shortcomings of Consent-Based Processing in Complex Situations

- Consent as a legal basis is not suitable when attempting to explain complex processes to data subjects, such as processing performed using AI tools, machine learning, or complicated algorithms that operate in a “black box” environment. In addition, even basic privacy policies worded in plain language are still often not understood (or even read) by data subjects, making consent an extremely complex issue in the direct marketing space and online more generally.

- While the importance of consent under the GDPR cannot be overstated, we must not ignore the clear standards established for securing GDPR-compliant consent. We do not want to run the risk of:

  - nullifying the protections intended for data subjects by “watering down” the requirements for compliant consent under the GDPR; or
  - removing societal benefits that could come from processing that is too difficult to explain at the time of data collection.

Benefits of MicroSegmentation

- A bridge is built between consent-based processing and Legitimate Interests-based processing by leveraging GDPR principles of Pseudonymisation and Data Protection by Design and by Default to technically enforce data access and boundaries.

- Data subject consent serves as the "centerpiece" of the puzzle, with other "pieces" (including Legitimate Interests as a legal basis) applied in situations where consent doesn’t apply, to allow for lawful processing. This can help to handle the complexity of the processing underlying data use in the direct marketing industry.

- A win-win combination of technical controls allows data controllers to process data, prove how they did it, *and* protect individual privacy rights, while achieving legitimate direct marketing business objectives in an ethical and lawful manner.

- Compliant direct marketing campaigns can scale at a global level. MicroSegmentation is not limited to solving GDPR compliance, as it is able to adapt to changes in data regulation globally. It also supports business objectives based on ethics and trust, completely separate from legal frameworks.

- Due to a clear pathway of data processing using technical controls, the data supply chain becomes more accountable and transparent for data subjects.

For more information go to MicroSegmentation.com

Anonos®

BigPrivacy® Unlocks Data

4 March 2020

Via Email: directmarketingcode@ico.org.uk

Direct Marketing Code Consultation Team
Information Commissioner's Office ("ICO")
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Re: Consultation - Draft ICO Direct Marketing Code of Practice ("Draft Code")

We appreciate the opportunity to participate in the public consultation on the Draft Code. Our aim is to assist in the ICO's goal of providing practical guidance and promoting good practice in relation to the processing for direct marketing purposes in compliance with data protection and e-privacy rules.

This feedback letter is submitted in our capacities as (i) Chief Strategist - Ethical Data Use, and (ii) Chief Executive Officer and General Counsel, of Anonos Inc. (www.anonos.com, "Anonos"). In lieu of providing responses to the specific questions identified in the ICO Consultation - Direct Marketing Code Draft Guidance, this comment letter provides feedback in narrative form due to the interrelated and overlapping nature of answers to the questions posed in the consultation.

As such, this letter takes the following approach.

I. First, we ask the ICO to address four questions for the benefit of society and industry.

II. Second, we propose a cooperative, trans-disciplinary approach to addressing the issues discussed in the Draft Code, and more generally.

III. Third, we highlight three "fictions" that are fundamental to overcoming misunderstandings related to:

   A. The relationship between the ICO and industry participants.
   B. Changing data privacy protection approaches.
   C. The role of the GDPR in reconciling conflicts between innovation and privacy.

IV. Fourth, we comment on several aspects of the GDPR's provisions and their application in the context of the Draft Code including:

   A. Lawful Basis for Processing Personal Data
   B. Shortcomings of Consent in Complex Situations

C. Benefits of Proper Legitimate Interests Processing
D. Purpose Limitation, Data Minimisation and Storage Limitation
E. Further Processing and the Compatible Purpose Test
F. Profiling and Automated Decision Making
G. GDPR Technical & Organisational Safeguards to Enable Lawful Direct Marketing
    1. Data Protection by Design and by Default
    2. Pseudonymisation

V. Fifth, as requested by the ICO, we present an example *of* direct marketing in practice, Anonos Microsegmentation, in which consent serves as the "centerpiece" of the puzzle, with other "pieces" (including, but not limited to, the Legitimate Interests legal basis) allowing for lawful data processing.

I. Questions For The Benefit Of Society And The Industry

For what we believe is ultimately for the benefit of both society and industry, we respectfully request clarification from the ICO in relation to the following questions:

1. May different legal grounds co-exist to support separate processes comprising lawful direct marketing, or must a single, unitary legal basis be established to support all end-to-end processing steps (e.g., collection, analytics, outreach, etc.) of personal data for direct marketing?

2. Can direct marketing itself serve as the purpose for which data is collected based on consent?

3. Can the further processing of personal data for direct marketing purposes be based on Legitimate Interests when supported by pseudonymised microsegments to respect and enforce the fundamental rights of data subjects?

4. Does all profiling necessarily constitute automated decision making?

II. Plea for Cooperative Trans-Disciplinary Approach

The General Data Protection Regulation ("GDPR"), as enacted in the UK via the Data Protection Act 2018 ("DPA"), is a complex and nuanced law. Numerous good faith interpretations of the GDPR will be put forward by different stakeholder groups until final determinations are made by the Court of Justice of the European Union ("CJEU").

The Draft Code has been introduced amidst concerns that industry has made no attempt to safeguard the fundamental rights of data subjects as well as counter-concerns that in the Draft Code the ICO inadvertently risks halting innovative uses of data.

We believe that to solve this issue in the midst of such discord and distrust, a trans-disciplinary approach should be taken, one in which both innovation and privacy rights can ultimately be respected. To that end, we highlight the following plea, originally published in the Duke Law & Technology review. This plea was raised in relation to some of the complications that come from complex processing such as ML and AI, which play a core role in the direct marketing industry issues that the ICO is trying to solve through the Draft Code:

> "We thus [reiterate] the common plea for collegiate work not only across different legal jurisdictions and across different disciplines, but also between academics and

practitioners. In relation to applied domains in particular, we fear that the situation is becoming more adversarial than collaborative, and that colleagues risk burning bridges with the very practitioner communities they should be working with, rather than against. Only with continuing trans-disciplinary collaboration can we hope not just to enslave the algorithm, but to create a more legitimate, more comprehensible and in the end more useful algorithmically-mediated society."[1]

III. Fictions in the Industry

Three fundamental "fictions" must be dispelled before real progress can be made in achieving a trans-disciplinary collaboration. We believe this kind of collaboration is critical if the goal is to balance data innovation for the benefit of society with the protection of fundamental rights for the benefit of individual data subjects.

A. Fiction #1: The ICO and other DPAs are trying to stop innovative uses of data.

Reality: The ICO and other Data Protection Authorities ("DPAs") are not looking to stop innovative uses of data. Rather, they are looking to interpret and enforce the GDPR. The GDPR itself states that "the processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."[2]

The ICO's enforcement and interpretation of the GDPR will by design inform innovative uses of data, but ultimately a balance is intended to be struck between the major benefits of data use, and the protection of data subject rights. Action by the ICO to preserve both of these goals will clearly support the aims and intentions of the GDPR.

B. Fiction #2: Traditional technologies for protecting data continue to work in today's world of ever-increasing volume, variety and velocity of data ("Big Data").

Reality: In most situations, technologies for protecting data in use that were previously effective before Big Data processing (and accompanying breaches) now fail to adequately protect data.[3] If organizations want to benefit from the repurposing, sharing, and combining of data at the scale and speed that Big Data enables, they must make changes to their processing of personal data to more effectively balance data innovation and protection of data subject interests and rights. To that end, they must adopt newly defined GDPR technical and organisational safeguards, particularly with regard to data in use.

C. Fiction #3: The GDPR does not provide the means to reconcile conflicts between data protection and innovation.

Reality: The GDPR leverages several decades of accumulated legislative, regulatory, and judicial experience to introduce new concepts to help balance data protection and innovation. Key among these are the following new technical and organisational

[1] Edwards, Lilian and Veale, Michael, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For (May 23, 2017). 16 Duke Law & Technology Review 18 (2017). Edwards, Lilian and Veale, Michael, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For (May 23, 2017). 16 Duke Law & Technology Review 18 (2017). https://ssrn.com/abstract=2972855 at 84.
[2] GDPR Recital 4.
[3] See https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html?smid=nytcore-ios-share

> safeguards defined legally for the very first time at the EU level – Data Protection by Design and by Default[4] and Pseudonymisation.[5] However, the requirements for these new technical and organisational safeguards must be strictly interpreted and enforced in accordance with the new definitions provided in the GDPR – *and not interpreted in accordance with pre-GDPR concepts and practice* – if the desired reconciliation of data protection and innovation is to occur.

If the goal is to achieve a trans-disciplinary collaboration to balance data innovation and protection, the above-noted fictions must first be dispelled. With this objective in mind, the following comments are hereby respectfully submitted to the ICO.

IV. Draft Code and Discussion on Relevant GDPR Provisions and Concepts

We would first like to highlight several relevant GDPR provisions and concepts that play a role in the legal and technical morass that the ICO is currently dealing with. We examine the process of determining a lawful basis for processing personal data, some issues with the legal ground of consent, and then look at the potential of Legitimate Interests processing. We then move to discuss GDPR concepts such as purpose limitation and data minimisation, secondary processing, and technical and organisational controls.

We then conclude with an example *o*f direct marketing in practice, Anonos Microsegmentation, that we believe provides support and clarity in finding a way through the myriad of the issues discussed below.

A. Lawful Basis for Processing Personal Data

An honest assessment of the current situation leads to the conclusion that historically, processing under the legal ground of Legitimate Interests has been misused and misapplied for processing personal data to the benefit of data controllers and the detriment of data subjects. A number of key industry players and commentators, including Privacy International, Brave, and the IAB, have noted that:

> "…it is self-evident that companies cannot treat their business needs / the pursuit of their business models as synonymous with 'legitimate interests'. The mere fact that a data controller may desire to engage in intrusive profiling in order to make money off its services is not sufficient. As Recital (47) of GDPR makes clear, what is legitimate should turn at least in part on whether a legitimate interest is served due to the relationship between the controller and subject."[6]
>
> "The tracking industry has misused legitimate interest for years."[7]
>
> "[We] have created a messy and frightening marketplace built on the collection and use of personal information that scares the daylights out of a lot of people because they don't understand it and cannot control it. We've built it in a way that requires a doctorate in

[4] See GDPR Recitals 78, 108 and Articles 25 and 47(2)(d).

[5] See GDPR Recitals 26, 28, 29, 75, 78, 85, 156, and Articles 4(5), 6(4)(e), 25(1), 32(a), 40(2)(d), and 89(1).

[6] Privacy International; see https://privacyinternational.org/sites/default/files/2018-11/08.11.18 Final Complaint Acxiom %26 Oracle.pdf at 28.

[7] Johnny Ryan, chief policy officer at Brave; see https://iapp.org/news/a/critics-on-croatias-eprivacy-proposal-legitimate-interest-provisions-not-legitimate

> engineering to understand. Governments have rightly stepped in to attempt to offer fixes, but their laws also are difficult to comprehend, by consumers and businesses alike."[8]

This prior improper behavior, however, does not justify the revocation of the rights of current and future data controllers. They should still be able to avail themselves of the different legal bases available to them under the GDPR, PECR and the e-privacy Directive (and eventually the e-privacy Regulation), as applicable to their specific circumstances. The following quote speaks to the trans-disciplinary collaboration necessary to balance data innovation and protection:

> "I personally think that after so many years of flawed cookie consent, it is a productive thing to do to introduce another approach into the legislative debate. My view is that 'legitimate interests' is misunderstood and underrated as a regulatory mechanism to protect our privacy."[9]

The Draft Code provides inconsistent guidance regarding the availability of Legitimate Interests as a lawful basis to process personal data related to direct marketing.

The Draft Code is correct that PECR and the e-privacy Directive (and potentially the e-privacy Regulation) require consent for some methods of direct marketing. However, as noted below it is not correct that the same legal basis must be used for all of the various processes that may be associated with direct marketing.

The Draft Code accurately describes the situation with the comment:

> "Generally speaking the two lawful bases that are most likely to be applicable to your direct marketing purposes are consent and legitimate interests. However it is important to remember that neither of these lawful bases are the 'easy option' and both require work."

It is certainly true that consent and Legitimate Interests both "require work" to ensure compliance with GDPR requirements.

However, the following quotes from the Draft Code leave the incorrect impression that: (i) assuming compliant consent is secured for lawful collection of personal data, the basis of Legitimate Interests is <u>not</u> available to support further processing of the data even if data subjects are put on proper notice at the time of collection and all underlying requirements are satisfied; and (ii) only one legal basis (consent) is available to support all of the various processes associated with direct marketing.

> "PECR requires consent for some methods of sending direct marketing. If PECR requires consent, then processing personal data for electronic direct marketing purposes is unlawful under the GDPR without consent. If you have not got the necessary consent, you cannot rely on legitimate interests instead. You are not able to use legitimate interests to legitimise processing that is unlawful under other legislation." *(emphasis added)*

> "If you have obtained consent in compliance with PECR (which must be to the GDPR standard), then in practice consent is also the appropriate lawful basis under the GDPR. Trying to apply legitimate interests when you already have GDPR-compliant consent would be an entirely unnecessary exercise, and would cause confusion for individuals."

[8] IAB, see https://www.iab.com/wp-content/uploads/2020/02/IAB_The-Great-Collab_ALM-2020-Keynote-Script.pdf at 8

[9] Eduardo Ustaran - Hogan Lovells Privacy and Cybersecurity Practice Global Co-Head; see https://iapp.org/news/a/critics-on-croatias-eprivacy-proposal-legitimate-interest-provisions-not-legitimate

> “Remember if PECR requires consent then in practice it is consent and not legitimate interests that is the appropriate lawful basis.”
>
> “It is unlikely that you will be able to apply legitimate interests for intrusive profiling for direct marketing purposes. This type of profiling is not generally in an individual’s reasonable expectations and is rarely transparent enough.”
>
> “Even if you are not using cookies, it is likely that consent will be the appropriate lawful basis under the GDPR for any behavioural advertising or profiling that you wish to engage in for the same reasons as online advertising more generally.”

The GDPR provides for the right to use different legal bases for different processes that relate to the same data. This is highlighted in ICO Guidance - *Lawful basis for processing* - as follows:

> “How do we decide which lawful basis applies?
>
> This depends on your specific purposes and the context of the processing. You should think about why you want to process the data, and consider which lawful basis best fits the circumstances. … You might consider that more than one basis applies, in which case you should identify and document all of them from the start. You must not adopt a one-size-fits-all approach. No one basis should be seen as always better, safer or more important than the others, and there is no hierarchy in the order of the list in the GDPR.
>
> In other cases you are likely to have a choice between using legitimate interests or consent.
>
> You may prefer to consider legitimate interests as your lawful basis if you wish to keep control over the processing and take responsibility for demonstrating that it is in line with people’s reasonable expectations and wouldn’t have an unwarranted impact on them. On the other hand, if you prefer to give individuals full control over and responsibility for their data (including the ability to change their mind as to whether it can continue to be processed), you may want to consider relying on individuals’ consent.
>
> It may be possible that more than one basis applies, in which case you should identify and document all of them from the start.”[10]

The GDPR explicitly recognizes that a number of different legal grounds may co-exist, provided that the requirements for each legal basis are satisfied.

The statement in GDPR Article 17(1) that “…and where there is no other legal ground for the processing…” suggests that “other” legal grounds may exist parallel to consent.

In addition, in its Guidance - *Guidelines on consent under Regulation 2016/679* - the EDPB writes:[11]

> “As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent - and in accordance with the GDPR - remain lawful, however, the controller must stop the processing actions

[10] See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

[11] During its first plenary meeting, the European Data Protection Board endorsed the WP29 Guidelines on consent under Regulation 2016/679, WP259 rev.01.

> concerned. If there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted by the controller."[12]

This supports the existence of multiple legal grounds for a single processing activity, or multiple connected processing activities that require different legal grounds for each portion.

Accordingly, so long as:

1. GDPR-compliant consent is in place for purposes of the initial collection of personal data;

2. Data subjects are put on proper notice of the use of non-consent legal bases; and

3. The requirements of such non-consent legal bases are satisfied;

then a non-consent legal basis, including Legitimate Interests, should remain available for use.

B. Shortcomings of Consent in Complex Situations

A critical consideration to note is that there are a number of situations in which consent as a legal basis for processing fails. One of the first issues is the requirement that information provided to data subjects must be clear and easy to understand.

This creates several issues when attempting to explain complex processes to data subjects, such as processing performed using AI tools, machine learning processes, or complicated algorithms that operate in a "black box" environment. In addition, even basic privacy policies or statements worded in plain language are still often not understood (or even read) by data subjects, making consent an extremely complex issue in the direct marketing space and online more generally.

While the importance of consent under the GDPR cannot be overstated, we must not ignore the clear standards established for securing GDPR-compliant consent. We do not want to run the risks of (i) nullifying the protections intended for data subjects by "watering down" the requirements for compliant consent under the GDPR, including requiring that the data subject is sufficiently informed and aware of what they are agreeing to, and (ii) removing from the global data ecosystem all societal benefits from processing that is too difficult to explain at the time of data collection.

The following commentary highlights this predicament:

> "The underlying logic of data-processing operations and the purposes for which they are used have now become so complex that they can only be described by means of intricate privacy policies that are simply not comprehensible to the average citizen because of both their content and their excessive length. The result is that hardly anybody reads these privacy policies. This complexity renders individuals powerless and fosters indifference, with the result that many people simply click "OK" when using online services."[13]

> "The torrent of data being generated from and about data subjects imposes an undue cognitive burden on individual data subjects. Overwhelming them with notices is ultimately disempowering and ineffective in terms of protection — it would take the average person

[12] WP259 rev.01 Article 29 Working Party Guidelines on consent under Regulation 2016/679 at 22
[13] Moerel & Prins, Privacy for the Homo Digitalis, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123 at 9.

> about 250 working hours every year, or about 30 full working days — to actually read the privacy policies of the websites they visit in a year."[14]

> "Another challenge of relying on consent is that convenience and people's limited capacity to make rational decisions prevent people from seriously spending time and intellectual effort on reading the privacy statements of every website, app, or service they use….the simpler you make the consent procedure, the less will users understand what they actually consent to; and the more meaningful you make the consent procedure (providing sufficient information about what will happen with the data), the less convenient the consent will become."[15]

> "Irrational behaviour means, in the end, that citizens do not always make a rational decision, partly due to lack of time, a short-term horizon or insufficient knowledge. The long and often complex privacy agreements that service users often agree to without reading them, are an example here."[16]

If consent is the only basis on which information for these purposes can be processed we face a Hobson's Choice:[17]

- "uninformed consent", which is a fiction we tell each other to make everyone feel better but places all the risk on the data subject, or

- no collection or processing at all for any complex research (health, scientific, marketing or otherwise) simply due to the complexity in explaining what is happening behind the scenes.

C. Benefits of Proper Legitimate Interests Processing

The foregoing limitations of consent in complex processing situations is one of the reasons that Legitimate Interests exists as an alternate legal basis. ICO Guidance - *What is the 'legitimate interests' basis?* - noted that:

> "Legitimate interests is different to the other lawful bases as it is not centred around a particular purpose (eg performing a contract with the individual, complying with a legal obligation, protecting vital interests or carrying out a public task), and it is not processing that the individual has specifically agreed to (consent). Legitimate Interests is more flexible and could in principle apply to any type of processing for any reasonable purpose.
>
> Because it could apply in a wide range of circumstances, it puts the onus on you to balance your legitimate interests and the necessity of processing the personal data against the interests, rights and freedoms of the individual taking into account the particular circumstances. This is different to the other lawful bases, which presume that your interests and those of the individual are balanced."[18]

[14] World Economic Forum Report: Unlocking the Value of Personal Data: From Collection to Usage, http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf at 11. See also note 13, *supra.*

[15] Koops, "The trouble with European Data Protection Law," International Data Privacy Law, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692 at 4. See also Moerel & Prins, Privacy for the Homo Digitalis, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123.

[16] See Dutch Minister of Economic Affairs in a letter on Big Data and Profiling. Parliamentary Documents II, 2014/15, 32761, nr. 78, p. 4. See also Moerel & Prins, Privacy for the Homo Digitalis, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123.

[17] See https://www.merriam-webster.com/dictionary/Hobson%27s%20choice

[18] See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

The Draft Code highlights the following requirements for Legitimate Interests as a processing ground for direct marketing.

> “The legitimate interests lawful basis is made up of a three-part test:
>
> - Purpose test – is there a legitimate interest behind the processing?
> - Necessity test – is the processing necessary for that purpose?
> - Balancing test – is the legitimate interest overridden by the individual’s interests, rights or freedoms?
>
> We refer to this test as a legitimate interests assessment (LIA). You must objectively consider whether legitimate interests apply to your direct marketing purposes.
>
> Recital 47 of the GDPR says: “…The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.”
>
> It is important to note that the GDPR says that direct marketing may be a legitimate interest. It does not say that it is always a legitimate interest and it does not mean that you are automatically able to apply this lawful basis to your direct marketing. Whether you can apply it depends on the particular circumstances.
>
> The fact that direct marketing ‘may be regarded’ as a legitimate interest is likely to help you demonstrate the purpose test, as long as the marketing is carried out in compliance with e-privacy laws and other legal and industry standards.
>
> You still need to show that your processing passes the necessity and balancing tests. You may also need to be more specific about your purposes for some elements of your processing in order to show that processing is necessary and to weigh the benefits in the balancing test. For example, if you use profiling to target your marketing.”

The above quotes from the Draft Code highlight the importance of satisfying all three of the tests required for lawful Legitimate Interests processing. The Purpose, Necessity and Balancing tests must *all* be satisfied, and “high marks” in one or more tests does *not* overcome the failure to satisfy other tests.

As a result, attempts to use Legitimate Interests processing for data uses that violate GDPR, including Article 5 (Principles Relating to Processing of Personal Data), such as discrimination against protected categories of individuals, illegally influence the results of elections, etc. will fail the first test. These data uses would not be lawful under Legitimate Interests grounds regardless of the outcomes of the Necessity and Balancing tests.

If a proposed data use satisfies both the Purpose and Necessity tests, then the Balancing test must be applied to assess the impact of the use on the interests and fundamental rights and freedoms of data subjects. In performing the assessment of relevant “impact”, the Article 29 Working Party has stated:

> “The Working Party emphasises that it is crucial to understand that relevant 'impact' is a much broader concept than harm or damage to one or more specific data subjects. 'Impact' as used in this Opinion covers any possible (potential or actual) consequences of

> the data processing. For the sake of clarity, we also emphasise that the concept is unrelated to the notion of data breach and is much broader than impacts that may result from a data breach. Instead, the notion of impact, as used here, encompasses the various ways in which an individual may be affected - positively or negatively - by the processing of his or her personal data."[19]

The need to assess the collective interests at stake on both sides of the balancing of interests equation – i.e., the interest of the data controller (or third party) and the interests of the data subject – are affirmed in opinions of the Article 29 Working Party and decisions of the CJEU. They note that "the clear signal is that collective interests must also be involved in these considerations. Only then can full account be taken of the constitutional basis for personal data protection at the EU level."[20]

The Draft Code includes the following statement under the heading "How does legitimate interests apply to direct marketing?":

> "If you do not need consent under PECR, then you might be able to rely on legitimate interests for your direct marketing purposes if you can show the way you use people's data is proportionate, has a minimal privacy impact and is not a surprise to people or they are not likely to object to what you are doing."

The above statement is confusing since date controllers will always need consent under PECR – at least for the initial data collection.

The ICO should clarify this statement to make it clear that the analysis of the availability of Legitimate Interests should only occur *after* the satisfaction of baseline PECR consent requirements. Once these PECR requirements have been satisfied for the initial collection of the data, Legitimate Interests processing is *then* available for evaluation.

D. Purpose Limitation, Data Minimisation and Storage Limitation

Another core issue exists surrounding the concepts of purpose limitation and data minimisation. These concepts play a major role in discovering a potential balance between industry goals and individual data subject privacy rights.

The Draft Code correctly highlights the following in the context of GDPR Articles 5(1)(b) Purpose Limitation, 5(1)(c) Data Minimisation and 5(1)(e) Storage Limitation:

> "The business opportunities created by profiling, cheaper storage costs and the ability to process large amounts of information can encourage organisations to collect more personal data than they actually need, in case it proves useful in the future. Controllers must make sure they are complying with the data minimisation principle, as well as the requirements of the purpose limitation and storage limitation principles.

[19] See Article 29 Working Party 06/2014 at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf at 35.

[20] See Moerel & Prins, Privacy for the Homo Digitalis, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123 at 36; citing Case C-131/12 Google Spain and Google Inc. May 13, 2014, EU:C:2014:317; Case C-362/14, Schrems, October 6, 2014, EU:C:2015:650; Opinion WP29 06/2014; Kranenborg, H.R. - Verhey, L.F.M. (2011), Wet bescherming persoonsgegevens in Europees, Kluwer; and Hijmans, H. (2016), What the EU does and should do to make Article 16 TFEU work, by means of judicial review, legislation, supervision by independent authorities, cooperation of the authorities and external action, diss. Universiteit van Amsterdam (handelseditie te verschijnen bij Springer Verlag).

> Controllers should be able to clearly explain and justify the need to collect and hold personal data, or consider using aggregated, anonymised or (when this provides sufficient protection) pseudonymised data for profiling.
>
> Machine-learning algorithms are designed to process large volumes of information and build correlations that allow organisations to build up very comprehensive, intimate profiles of individuals. Whilst there can be advantages to retaining data in the case of profiling, since there will be more data for the algorithm to learn from, controllers must comply with the data minimisation principle when they collect personal data and ensure that they retain those personal data for no longer than is necessary for and proportionate to the purposes for which the personal data are processed
>
> The controller's retention policy should take into account the individuals' rights and freedoms in line with the requirements of Article 5(1)(e)."

The GDPR principle of purpose limitation,[21] with its origins in international standards developed by the OECD[22] and the Council of Europe,[23] reflects the rights articulated in Article 8(2) of the Charter of Fundamental Rights of the European Union as follows:

> "These data must be processed fairly, for specified purposes, and with the consent of the individuals to which they relate or on the basis of some other legitimate basis laid down by law."

The GDPR principles of data minimisation[24] and storage limitation[25] are linked to purpose limitation in that no more data may be processed, or stored for longer, than necessary for the purpose stated at the time of data collection. In the past, the collection or processing of personal data was primarily a by-product of the primary purpose for which the data was collected.

In this circumstance, if the purpose of data collection is not the same as the purpose of the desired data processing, then the GDPR principles of purpose limitation, data minimisation and storage limitation would prohibit lawful processing of the personal data.[26]

One potential approach for enabling lawful expanded use of data for direct marketing purposes in a manner consistent with the expectations and consent of data subjects is described in detail in *Anonos Microsegmentation in Support of Direct Marketing* below. In brief, our suggested approach combines (among other things):

- Obtaining consent to data collection for direct marketing purposes.
- Using Legitimate Interests for further processing of the collected data for direct marketing.
- Creating privacy-respectful segmented datasets using anonymisation and pseudonymisation techniques, enhanced with both recommended and innovative improvements[27] as technical

[21] GDPR Article 5(1)(b).
[22] See Section 9 of the OECD, 1980: "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."
[23] See Article 5(b) of the Council of Europe, 1981.
[24] GDPR Article 5(1)(c).
[25] GDPR Article 5(1)(e).
[26] But see discussion below regarding lawful further processing if the "compatible use" test is satisfied.
[27] See www.anonos.com/ENISAguidelines

controls. This will ensure adequate mitigation of risks to data subject interests and rights and help satisfy the requirements of the balancing of interests test in favor of the processing.

E. Further Processing and the Compatible Purpose Test

We believe that the Draft Code should discuss the lawfulness of further processing of personal data under certain conditions for purposes of direct marketing.

Under GDPR Article 6(4), personal data collected on the basis of Legitimate Interests, a contract or vital interests may be further processed for another purpose if the new purpose is compatible with the original purpose. The European Commission in its guidance - *Can we use data for another purpose?* **-** highlights the following points (as stated in the GDPR) as being relevant for determining whether a new purpose is compatible with the original purpose:[28]

- the link between the original purpose and the new/upcoming purpose;
- the context in which the data was collected (what is the relationship between a data controller and the individual?);
- the type and nature of the data (is it sensitive?);
- the possible consequences of the intended further processing (how will it impact the individual?); and
- the existence of appropriate safeguards (such as encryption or pseudonymisation).

In addition, they also note that if a data controller wants to use the data for statistical or scientific research “it is not necessary to run the compatibility test.”

Furthermore, the European Commission guidance[29] states that if a data controller has collected the data “on the basis of consent or following a legal requirement, no further processing beyond what is covered by the original consent or the provisions of the law is possible.” In these instances, “further processing would require obtaining new consent or a new legal basis.”

This underscores the “Hobson’s Choice” noted above: if the processing is too complex to explain simply, (or too complicated to comprehend, but data subjects consent anyway, rendering the consent invalid) then either the processing cannot be allowed at all (with the attendant loss of societal benefits) or a non-consent legal basis must, in practice, actually be available for use.

F. Profiling and Automated Decision Making

Another issue we would like to highlight is the issue of profiling and automated decision-making. We believe that the difference between these terms is starting to become obscured, leading to confusion about the applicability of these concepts from a legal perspective.

The GDPR Article 22(1) prohibition on decision making “based solely on automated processing, including profiling, which produces legal effect concerning him or her or significantly affects him or

[28] See https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en
[29] Id.

her" was ported to the GDPR from Article 15(1) of the Data Protection Directive ("DPD"),[30] which itself was derived from France's 1978 Act on data processing, files and individual liberties.[31]

With one notable exception, neither DPD Article 15 nor GDPR Article 22 has to our knowledge been the subject of litigation before the CJEU or any national courts, nor have they figured prominently in enforcement actions by DPAs or assessments of the adequacy of third countries' data protection regimes.[32]

The one notable exception is the judgment by the German Federal Court of Justice in the so-called SCHUFA case[33] concerning the use of automated credit-scoring systems. In this case, the court held, on appeal, that the credit-scoring system fell outside the ambit of the German rules embodying DPD Article 15 because the automated elements of the decision-making process related only to the preparation of data. The court found that ultimately the actual decision to provide credit was made by a person.

We believe the Draft Code should include the following language from prior ICO guidance that further clarifies that:

1. Not all profiling is automated decision-making;

2. Automated decision-making is prohibited only if it "produces legal effect concerning a data subject or significantly affects the data subject"; and

3. A Data Protection Impact Assessment (DPIA) should be conducted when profiling to show that risks have been identified, assessed and mitigated.

The previous ICO guidance - *Rights related to automated decision making including profiling* - outlined that:

> "The [Article 22] restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effects are not defined in the GDPR, but the decision must have a serious negative impact on an individual to be caught by this provision.
>
> A legal effect is something that adversely affects someone's legal rights. Similarly significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.
>
> Because this type of processing is considered to be high-risk the GDPR requires you to carry out a Data Protection Impact Assessment (DPIA) to show that you have identified and assessed what those risks are and how you will address them.
>
> What if Article 22 doesn't apply to our processing?

[30] See Articles 12(a) and 15 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[31] Loi no. 78-17 du 6. janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[32] See Mendoza & Bygrave, The Right not to be Subject to Automated Decisions based on Profiling at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855 at 4.
[33] German Federal Court of Justice judgment of 28 January 2014, VI ZR 156/13.

Article 22 applies to solely automated individual decision-making, including profiling, with legal or similarly significant effects. If your processing does not match this definition then you can continue to carry out profiling and automated decision-making.

"But you must still comply with the GDPR principles."[34]

G. GDPR Technical & Organisational Safeguards to Enable Lawful Direct Marketing

In order to advance the trans-disciplinary collaboration necessary to balance data protection and innovation, the Draft Code should be expanded to address more than "data protection by design" to include a description of the full requirements of Data Protection by Design and by Default, as newly defined in Article 25 of the GDPR.

In addition, we (as the audience for the Draft Code) would benefit greatly from a description of the requirements and benefits of "Pseudonymisation" as newly defined in Article 4(5) of the GDPR.

The combination of GDPR-compliant Data Protection by Design and by Default and Pseudonymisation could assist greatly in enabling readers of the Draft Code to ensure lawful direct marketing activities.[35]

1. Data Protection by Design and by Default

We respectfully disagree with the ICO's statement in the guidance - *Data Protection by Design and Default Principles* - linked to on page 26 of the Draft Code that:

- [Data protection by design and by default] is not new. Previously known as 'privacy by design', it has always been part of data protection law. The key change with the GDPR is that it is now a legal requirement.

- Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability.[36]

Contrary to the ICO guidance language quoted above, the GDPR requires more than just Privacy by Design.[37]

Data Protection by Design and by Default, as newly defined under GDPR Article 25, goes beyond Privacy by Design. An important element of Data Protection by Design and by Default is that the limits and requirements applicable to data processing must be built into the technology itself.[38]

[34] See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

[35] Anonos is a founding member of the 5th Cookie working group (see www.5thCookie.com) which was established to support exploration of using GDPR recommended technical and organisational safeguards – like Data Protection by Design and by Default and Pseudonymisation – to enforce greater accountability and ethics across the AdTech real-time bidding (RTB) ecosystem. See also https://www.pseudonymisation.com/ for additional information on the benefits of GDPR compliant Pseudonymisation.

[36] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

[37] Privacy by Design is the approach championed by Ann Cavoukian, Ph.D., former Information and Privacy Commissioner of Ontario, for embedding privacy into the system design process. See https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[38] Moerel & Prins, Privacy for the Homo Digitalis, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123 at 82.

The GDPR requires that Data Protection by Design and by Default be applied at the earliest opportunity (e.g., by pseudonymising data at the earliest opportunity) to limit data use to the minimum extent and time necessary to support each specific product or service authorized by an individual data subject.[39] This is a more stringent standard than basic Privacy by Design, which is simply “considering data protection and privacy issues upfront in everything you do.”

Encryption and traditional Privacy Enhancing Techniques (PETs) were developed long before the GDPR requirements were established. When used alone, encryption and PETs will likely fail to satisfy new GDPR Data Protection by Design and by Default requirements.

For example, static tokens and identifiers used for marketing purposes such as “the ‘Google Advertising ID’ (ADID), the ‘Identifier for Advertising’ (IDFA) on iOS and the ‘Advertising ID’ on Windows 10” highlighted on page 95 of the Draft Code fall short of requirements for Data Protection by Design and by Default because links between data subjects and identifying information are readily ascertainable.

The Draft Code highlights this danger in the statement on page 95 that:

> “Whilst often described as an ‘anonymous identifier’, an advertising ID forms an example of an ‘online identifier’ which Recital 30 of the GDPR states can be personal data.”

DPAs are likely to conclude that static tokens and identifiers used for marketing purposes fail to satisfy GDPR Data Protection by Design and by Default requirements because of the risk of unauthorized re-identification via the Mosaic Effect. The Mosaic Effect occurs when a person is indirectly identifiable via linkage attacks because information can be combined with other pieces of information, enabling the individual to be distinguished from others.[40]

These static tokens and identifiers will not satisfy the requirements for GDPR-compliant Pseudonymisation if personal data can be attributed to specific data subjects without the use of separately kept “additional information.” This means that the benefits enumerated below associated with properly Pseudonymised data will not be available under the GDPR.

Finally, stateless tokens[41] developed for PCI compliance in the payment card industry fail to enforce re-linking and revealing of personal data under the controlled conditions necessary to support iterative analytics, including the secondary uses of data necessary to support lawful direct marketing.

Data Protection by Design and by Default leverages incentives built into the GDPR to use technical and organisational measures for compliant secondary use of data that could enable lawful direct marketing.

2. Pseudonymisation

One of the technical and organisational measures set out in the GDPR is Pseudonymisation, as newly-defined in Article 4(5).[42]

[39] See GDPR Articles 15(1) and (2).

[40] See www.MosaicEffect.com

[41] Stateless tokens are tokens that change frequently to replace identifying information.

[42] The definition of Pseudonymisation as now found in Article 4(5) of the GDPR was created roughly four years ago during the early drafting days of the GDPR. It requires that personal data must not be able to be attributed to a specific data subject without the use of additional information kept separately, and subject to technical and organisational measures.

The GDPR provides incentives to use technical and organisational measures, including Pseudonymisation, to enable the flow, commercial use, and value maximization of data in a way that recognizes, respects, and enforces the fundamental rights of individuals.
Pseudonymisation involves the separation of the information value derived from processing activities from the ability to re-identify data subjects using direct or indirect identifiers. The definition also requires that re-identification can only occur via access to separately stored "Additional information" in support of authorised purposes.[43]

The use of GDPR-defined Pseudonymisation helps to:

A. **Support Lawful Data Repurposing, Sharing and Combining**

   a. Lawful Repurposing, Sharing and Combining.

      i. Pseudonymisation is explicitly highlighted in GDPR Article 6(4)(e) as an "appropriate safeguard" that can be used by data controllers "in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected."

   b. Protect Data In Use When Consent Is Not Available.

      i. Properly-Pseudonymised data is recognized in the Article 29 Working Party Opinion 06/2014 as playing "…a role with regard to the evaluation of the potential impact of the processing on the data subject...tipping the balance in favour of the controller" to help support Legitimate Interest processing to protect data in use.[44]

      ii. The benefits of processing personal data using compliant Legitimate Interests processing as a legal basis under the GDPR include:

         1. Under Article 17(1)(c), if a data controller can show they "have overriding legitimate grounds for processing" supported by technical and organizational measures to satisfy the balancing of interest test, they have greater flexibility in complying with Right to be Forgotten requests.

         2. Under Article 18(1)(d), a data controller has flexibility in complying with claims to restrict the processing of personal data if they can show they have technical and organizational measures in place so that the rights of the data controller properly override those of the data subject because the privacy of the data subject is protected.

         3. Under Article 20(1), data controllers using Legitimate Interests processing are not subject to the right of portability, which applies only to consent-based processing.

[43] See www.MosaicEffect.com
[44] See https://dataprotectionmagazine.com/?p=975

4. Under Article 21(1), a data controller using Legitimate Interests processing may show they have adequate technical and organizational measures in place so that the rights of the data controller properly override those of the data subject because the rights of the data subjects are adequately protected. However, data subjects always have the right under Article 21(3) to *not* receive direct marketing outreach as a result of such processing.

B. Overcome Prohibitions Against Special Category Processing

a. Pseudonymisation helps to satisfy the Article 9(2)(g) exception to the general prohibition against the processing of special category data if the "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

b. Pseudonymisation helps to satisfy the Article 9(2)(i) exception to the general prohibition against the processing of special category data if the "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy."

c. Pseudonymisation helps to satisfy the Article 9(2)(j) exception to the general prohibition against the processing of special category data if the "processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) [which explicitly cites Pseudonymisation] based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

C. Separate Processing Benefits From Re-Identification Obligations

a. Pseudonymisation helps to enable Article 11(2) relaxation of obligations to data subjects under Articles 15 (Right of Access by Data Subject), 16 (Right to Rectification), 17 (Right to Erasure - Right to be Forgotten), 18 (Right to Restriction of Processing), 19 (Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing), and 20 (Right to Data Portability) when processing does not require identification when the data controller is not in a position to identify data subjects and the controller has informed data subjects accordingly. Data controllers not in possession of "Additional Information" necessary for re-identification satisfy this requirement.

b. Pseudonymisation helps to enable Article 12(2) relaxation of obligations under Articles 15 (Right of Access by Data Subject), 16 (Right to Rectification), 17 (Right to Erasure - Right to be Forgotten), 18 (Right to Restriction of Processing), 19 (Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing), and 20 (Right to Data Portability) in addition to the relaxation of obligations under Articles 21 (Right to Object to Automated Decision-Making) and 22 (Automated Individual Decision-Making, Including Profiling) to provide transparent information, communication and modalities for the exercise of the rights of the data subject when the data controller can demonstrate it is not in a position to identify data subjects. Data controllers not in possession of "Additional Information" necessary for re-identification satisfy this requirement.

c. *NB: See Anonos Microsegmentation in Support of Direct Marketing below.*

D. Maximise the Availability of Lawful Profiling and Digital Marketing

a. Pseudonymisation reduces the risk that profiling "produces legal effects concerning [data subjects] or similarly significantly affects [data subjects]" under Article 22(1) because it can be left up to the data subject whether to choose to participate in opportunities presented to them as a member of a Pseudonymised group. *See Anonos Microsegmentation in*

b. Pseudonymisation reduces the risk that profiling "decision[s are made] based solely on automated processing" under Article 22(1) because it can be left up to the data subject whether to choose to participate in opportunities presented to them as a member of a Pseudonymised group.

c. Pseudonymisation helps to enable Article 22(2)(b) support for processing "authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests."

d. Pseudonymisation helps to enable Article 22(4) allowance for decisions "based on special categories of personal data referred to in Article 9(1)" premised on Article 9(2)(g) Union or Member State laws by ensuring that "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

e. *NB: See Anonos Microsegmentation in Support of Direct Marketing below.*

E. Satisfy Data Protection by Design and by Default Obligations

a. Article 25(1) requires data controllers - for both primary and secondary processing - to "implement appropriate technical and organisational measures, such as pseudonymisation."

b. Pseudonymisation helps data controllers to satisfy their obligations under Article 25(2) to "implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."

F. Reduce the Risk of Data Breach Liability Obligations and Liability

a. Article 32 explicitly recognises Pseudonymisation and encryption as measures “[t]aking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."

b. Pseudonymisation helps to ensure that data breaches are “unlikely to result in a risk to the rights and freedoms of natural persons.” This would mean that an incident would not qualify as a data breach under GDPR and thus would not have to be notified to a supervisory authority under Article 33.

c. Pseudonymisation helps to ensure that data breaches are not “likely to result in a high risk to the rights and freedoms of natural persons.” This would mean that an incident would not qualify as a data breach under GDPR and/or (thus) would not have to be communicated to the data subject under Article 34.

G. Improve Scalability of Data Protection Impact Assessments

a. Pseudonymisation helps to satisfy Article 35(3)(b) obligations when “processing on a large scale of special categories of data referred to in Article 9(1).”

b. Pseudonymisation helps to satisfy Article 35(8) creation of and adherence to “approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.”

c. Pseudonymisation helps to enable Article 35(10) elimination of separate data protection impact assessment obligations under Articles 35(1)-(7) “[w]here processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis.”

H. Enable Benefits of Expanded Lawful Processing

a. Article 89(1) provides that “[p]rocessing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include Pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."

b. Article 89(1) Pseudonymisation-enabled processing enables greater flexibility under:
   i. Article 5(1)(b) with regard to purpose limitation;
   ii. Article 5(1)(e) with regard to storage limitation; and
   iii. Article 9(2)(j) with regard to overcoming the general prohibition on processing Article 9(1) special categories

V. Anonos Microsegmentation in Support of Direct Marketing

This discussion on Anonos Microsegmentation[45] is offered in response to the question asked in the ICO Consultation – Direct Marketing Code:

> *"Do you have any examples of direct marketing in practice, good or bad, that you think it would be useful to include in the code?"*

Anonos Microsegmentation is at the core of the 5th Cookie working group[46] proposal to use GDPR-recommended technical and organisational safeguards in digital marketing. The central 5th Cookie proposal is to leverage consent and Legitimate Interests, as well as enhanced pseudonymisation and anonymisation techniques to create privacy-respectful datasets containing "microsegments" that support compliant AdTech. Anonos Microsegmentation, however, extends beyond AdTech to apply to direct marketing, as well as applications in data processing more generally.

Anonos Microsegmentation leverages Anonos' technology, which transforms digital representations of people - or "Digital Twins" - into privacy-respectful "Variant Twins" of personal data by applying Pseudonymisation-enabled anonymisation techniques.[47] The resulting Variant Twins are use-case-specific, privacy-enhanced versions of Digital Twins. Privacy policies are embedded at the data element level, satisfying statutory and contractual requirements for lawful data use.[48] Variant Twins are ideal for creating privacy-respectful microsegments that support GDPR-compliant direct marketing, as explained below.

[45] See www.MicroSegmentation.com for more information.

[46] See note 35, *supra.*

[47] Newly defined GDPR compliant Pseudonymisation protects against negative effects from data breaches and prevents profiles from being used for decisions to communicate to an individual without the assessments required by Data Protection by Design and by Default as required by the GDPR. The European Union Agency for Cybersecurity (ENISA) has published two reports since the adoption of the new GDPR definition of Pseudonymisation on best practices for compliant pseudonymisation - in November 2018 (at https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions) and 2019 (https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices). EDPS Opinion 7/2015 on Meeting the Challenges of Big Data further highlights Pseudonymisation as playing "a role in reducing the impact on the rights of individuals, while at the same time allowing organisations to take advantage of secondary uses of data" at https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf at 15. A comparison of Anonos Pseudonymisation technology to ENISA published guidance on Pseudonymisation is available at https://www.anonos.com/enisa-guidelines.

[48] Anonos state-of-the-art Pseudonymisation technology enables lawful repurposing of data while preserving 100% accuracy to maximise data utility by expanding opportunities to ethically process, share and combine data in compliance with evolving data privacy regulations. Additional information about Anonos Pseudonymisation technology is available at www.anonos.com.

Anonos Microsegmentation – Benefits and Advantages

With Anonos Microsegmentation:

- Data subjects are presented with advertising offers in their capacity as members of small, dynamically-changing subgroups called microsegments. Based on their individual characteristics, data subjects can be included in multiple microsegments. The composition of microsegments changes dynamically, as new or updated data on data subjects results in their movement in or out, corresponding to the specified characteristics associated with the microsegment.

- Organisations can reach groups of people represented by microsegments in which they are interested. However, data subjects are approached as members of groups and not as individuals. It is up to each data subject to "raise their hand" if they want to respond to an offer. Crucially, at any time, data subjects can opt out of being included in further outreach based on microsegments.

- Compliant direct marketing campaigns can scale at a global level. Microsegmentation is not limited to solving GDPR compliance, as it is able to adapt to changes in data regulation globally. It also supports business objectives based on ethics and trust, completely separate from legal frameworks.

- The data supply chain becomes more accountable and transparent.

- Technical controls support data minimisation and purpose limitation, while reducing the scope of unnecessary data sharing, and alleviating privacy-related risks to data subjects.

- Data subject consent serves as the "centerpiece" of the puzzle, with other "pieces" (including, but not limited to, Legitimate Interests as a legal basis) applied in situations where consent doesn't apply, to allow for lawful processing. This can help to handle the complexity of the processing underlying data use in the direct marketing industry.[49]

- A bridge is built between consent-based processing and Legitimate Interests-based processing by leveraging GDPR principles of Pseudonymisation and Data Protection by Design and by Default to technically enforce data access and boundaries.

- A win-win combination of technical controls can allow data controllers to process data, prove how they did it, *and* protect individual privacy rights, while achieving legitimate direct marketing business objectives in an ethical and lawful manner.

- Auditable controls can be embedded into the process. This can allow oversight organisations and auditors to gain demonstrable insight into how processing has been performed, helping data controllers to reflect "demonstrable accountability" and meet GDPR requirements.

Anonos Microsegmentation enables direct marketing data ecosystem into which data subjects opt-in.

[49] Consent-based data collection and processing does not work in all circumstances - e.g., where processing cannot be described with sufficient detail at the time of data collection. For example, privacy notices may lack clarity, processing may be difficult to define, etc. The GDPR provides for an alternative legal basis for processing - which picks up where consent leaves off - to enable lawful processing in these situations if the requirements for Legitimate Interest processing are satisfied.

This helps to meet high regulatory standards for consent by enabling:

- Robust user controls;
- A compelling user engagement experience; and
- Strong technology-enforced privacy controls.

In doing so, Anonos Microsegmentation offers strong incentives for users to consent to data collection for the express purpose of being included in microsegments processed by the system.

They key to building trust whilst ensuring privacy is to encourage direct marketing models to evolve in ways that provide transparency and leverage technical and organisational safeguards to enforce privacy protection and to secure data subject rights. This opens up the possibility of broader reliance on legal bases such as Legitimate Interest to process personal data for direct marketing purposes.

Here too, Anonos Microsegmentation can support compliance. Its use of enhanced pseudonymisation, anonymisation techniques, and k-anonymity create strong technical safeguards that support the use of Legitimate Interests as a legal basis by reducing the risk to data subjects' rights. This risk is reduced to such a degree that the balancing test can be tipped in favor of the data controller, which allows greater flexibility in the processing of personal data for direct marketing.

Anonos Microsegmentation enables and enforces trust and ethical business practices. In addition, Anonos Microsegmentation can demonstrate to regulators that innovative technologies and new industry approaches can meet the rights and expectations of data subjects while allowing responsible data use.

- Anonos Microsegmentation is more privacy respectful and efficient than other approaches to direct marketing.
- Anonos Microsegmentation gives organizations access to the same advanced targeting with no decrease in insight accuracy.
- Individuals benefit from improved privacy and control over third-party access to and use of identifying information about them.

A trusted party handles the "last mile"[50] of data subject interaction to ensure that no identifying information about data subjects is revealed, except as specifically authorized by the data subjects. Using their relationship with the trusted party, data subjects can consent to receive relevant ads based on their inclusion in dynamically-changing and privacy-respectful microsegments.

The trusted third party has separately-stored information and secret keys necessary to "re-identify" individuals from within the microsegments for direct marketing purposes (this would be the "additional information" necessary under the GDPR Article 4(5) definition of Pseudonymisation required for authorized re-identification to occur). During processing, all personal data is pseudonymised and organised into privacy-respectful microsegments, and the processor during the microsegmentation process does not have access to the "additional information," keeping data subject privacy intact.

[50] The term "last mile" is used in the telecommunications, cable television and Internet industries to refer to the final leg of delivering communications to a retail customer.

The trusted party has a direct relationship with data subjects participating in the microsegmentation system and takes steps necessary to comply with data subject rights under the GDPR, including the following, as applicable:

- Article 12 - Transparent information, communication and modalities for the exercise of the rights of the data subject (including disclosure that personal data will be used to create 'lookalike' audiences, etc.).
- Article 13 - Information to be provided where personal data are collected from the data subject.
- Article 14 - Information to be provided where personal data have not been obtained from the data subject.
- Article 15 - Right of access by the data subject.
- Article 16 - Right to rectification.
- Article 17 - Right to erasure ('right to be forgotten').
- Article 18 - Right to restriction of processing.
- Article 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing.
- Article 20 - Right to data portability.
- Article 21 - Right to object.
- Article 22 - Automated individual decision-making, including profiling

Anonos Microsegmentation – The Details

The following is a more detailed explanation of how microsegments work to preserve privacy and data utility for direct marketing purposes.

This is accomplished as follows:

- A data controller first collects personal data for the express purpose of direct marketing after having obtained GDPR-compliant consent from a data subject with whom they have a direct relationship.
- Contemporaneous with obtaining consent, notice is provided of further processing for the express purpose of direct marketing based on Legitimate Interests. This notice describes the intended processing as well as the technical and organisational controls used to mitigate risks to data subjects' interests and rights.
- Collected data is immediately protected through a combination of anonymisation and enhanced pseudonymisation techniques that are applied not only to direct identifiers, but also to indirect identifiers, and in particular, those that are used to specify the schema(s) defining the microsegments.

  - These techniques are applied in compliance with GDPR requirements for Pseudonymisation[51] and Data Protection by Design and by Default[52] in accordance with guidelines by the European Union Agency for Cybersecurity (previously, the European Union Agency for Network and Information Security, ENISA).[53]

- The resulting privacy-protected "Variant Twins" are then shared by various data controllers with one or more trusted third parties for pooling into a combined dataset comprising large numbers of data subjects and a wide variety of microsegments. Importantly:

- Trusted third parties are explicitly and transparently identified as a joint-controller/data processor during the consent and Legitimate Interests notification processes.

- Pseudonyms used by each data controller are unique to their data subjects, and unique between Variant Twins they share with different trusted data partners.

- Data controllers hold the "additional information" needed to reattribute pseudonymised data to data subjects separately" but only for their own customers. Trusted third parties are in possession of the information held separately needed to create microsegments comprising data from multiple data controllers, and to do the re-identification necessary to present offers to data subjects on behalf of a party who wants to engage in targeted direct marketing.

- Data subjects have the express right to withdraw their consent to receive targeted direct marketing at any time.

* * * * *

As noted at the outset of this comment letter, we respectfully request clarification from the ICO in the form of answers to the following questions posed below:

1. May different legal grounds co-exist to support separate processes comprising lawful direct marketing, or must a single, unitary legal basis be established to support the end-to-end processing (collection, analytics, outreach, etc.) of personal data for direct marketing?

2. Can direct marketing itself serve as the purpose for which data is collected based on consent?

3. Can the further processing of personal data for direct marketing purposes be based on Legitimate Interests when supported by pseudonymised microsegments to respect and enforce the fundamental rights of data subjects?

4. Does all profiling necessarily constitute automated decision making?

[51] See GDPR Article 4(5).
[52] See GDPR Article 25.
[53] See www.anonos.com/ENISAguidelines

In closing, Anonos would like to express its sincere appreciation for the opportunity to submit this comment letter in response to Draft Code to provide practical guidance and promote good practice in regard to processing for direct marketing purposes in compliance with data protection and e-privacy rules.

We would also welcome the opportunity to discuss any of the foregoing at your convenience.

Respectfully Submitted,

Maggie

Gary

Magali ("Maggie") Feys
Chief Strategist - Ethical Data Use

M. Gary LaFever
CEO & General Counsel

Please email CommentLetters@anonos.com with any questions.